ASG Soft Key

Software Authentication Key

User Guide

Version 1.0

AVAYA, Inc.
211 Mt. Airy Rd.
Basking Ridge, NJ 07920
www.avaya.com

February 2003
Release 1.0

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no responsibility for any errors or liability for any direct or consequential damages resulting from use of the information. Changes and/or corrections to the information contained in this document may be incorporated into future issues.

Responsibility for Your System's Security

Toll fraud is the unauthorized use of your telecommunications system by an unauthorized party, for example, persons other than your company's employees, agents, subcontractors, or persons working on your company's behalf. Note that there may be a risk of toll fraud associated with your telecommunications system, and if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

You and your System Manager are responsible for the security of your system, such as programming and configuring your equipment to prevent unauthorized use. The System Manager is also responsible for reading all installation, instruction, and system administration documents provided with this product to fully understand the features. Avaya Inc. will not be responsible for any charges that result from the unauthorized use of your system.

Trademark Notice

Avaya is a registered trademark of Avaya, Inc.

Home Page

The home page for Avaya, Inc. is http://www.avaya.com.

To Get Help

If you need assistance with administration of the ASG Guard/ASG Guard Plus call Avaya, Inc. at **1-800-242-2121**, or your local Authorized Dealer. Avaya's technical support staff is available 24 hours. This call may be billable.

Fraud Intervention

If you suspect you are being victimized by toll fraud and you need technical support or assistance, call Avaya Customer Care at 1-800-242-2121, or your local authorized dealer. For international customers, contact your local Center of Excellence.

Table of Contents

1. Welcome!

The ASG Soft Key is a software utility that enables you to establish secure user sessions with Avaya infrastructure security appliances.

The ASG Soft Key relies on *Two-Factor Authentication* – a security process that confirms your identity based on two distinctive factors: something you have (your software token) and something you know (your user PIN). A simple example of two-factor authentication is an individual's ATM (Automated Teller Machine) card and his or her PIN (Personal Identification Number). Independently, these items are useless to a prospective identity thief. Only when appropriately used together is identity confirmed and access granted.

With the ASG Soft Key, the factor that you know is the *PIN* you have selected, and the factor that you have is called a *token*. Tokens are unique and not easily replicable; and access rights can be revoked at any time. They are available as hardware or software tokens.

The ASG Soft Key is designed to emulate hardware tokens such as the ASG Key. The ASG Soft Key operates in a Microsoft Windows (98/NT/2000) environment as well as on mobile platforms such as the Palm™ handheld and BlackBerry™ wireless handhelds. Software tokens provide the same functionality as hardware tokens, and eliminate the need to carry an extra piece of equipment.

The ASG Soft Key operates in the *Challenge/Response* authentication mode. Authentication tokens are always associated with a user profile on the destination appliance. Within this profile a user key is defined and that key is then seeded into the authentication token. When the user logs into the appliance, the appliance issues a numeric challenge that is entered into the token, and the token generates a numeric response that is entered into the host for successful authentication.

1.1 Document Overview

This guide explains how to use the ASG Soft Key on all available operating platforms, to authenticate to security appliances and software.

After reading this document, you should be able to:

- Install the ASG Soft Key and configure your settings on all available operating platforms.
- Add a user profile to a destination appliance that corresponds to the ASG Soft Key authentication method.
- Use the soft token to successfully authenticate into ASG security appliances.

1.2 Audience Assumptions

This document assumes its audience has an understanding of ASG appliances, and is familiar with authentication processes for accessing these products. User should also know how to use software applications within a Microsoft Windows environment, or one of the mobile operating platforms referred to in this guide.

1.3 Document Conventions

This document observes the following conventions:

- Screen and icon names and section titles are **bold**.
- Keyboard keys are shown in CAPS.
- Selectable screen items such as buttons or links are shown in “quotations.”
- Successive menu selections are **bold**, and displayed with the › (greater than) symbol. For instance: Select **File > Configure**.

	Notes provide useful information in addition to any given topic.
	Tips provide alternate operations, hints, and/or timesaving suggestions.
	Warnings provide critical information that you must be aware of as you proceed to use your software.

1.4 Related Reading Material

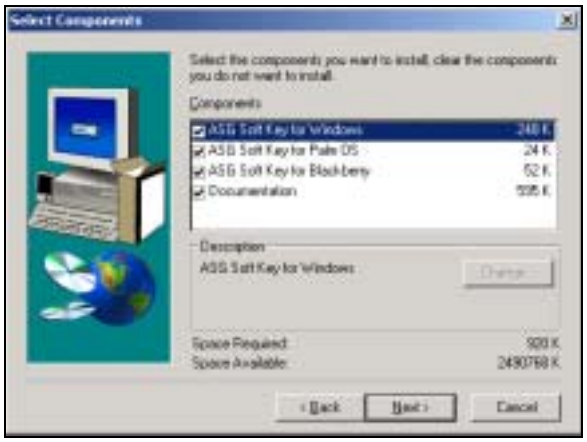
Since you will be using the ASG Soft Key in conjunction with one of several other ASG products, related reading material includes the user guide that accompanies the ASG product to which you are authenticating. If you are using the ASG Soft Key on a handheld, you should refer to the user documentation that accompanied your device for basic operating and installation information.

2. Getting Started

To get started with the ASG Soft Key, you will need to install the software, familiarize yourself with its interface and features. This section provides instructions for installing the ASG Soft Key on all supported platforms, and provides an overview of its interface and features.

2.1 Installing the ASG Soft Token in Microsoft Windows

1. Locate the **ASGSoftKey.exe** file and double-click to begin installation; the **Avaya** splash screen briefly displays, then the installation software **Welcome** screen displays.
2. Click "Next" to continue; the **Software License Agreement** displays.
3. Press "Yes" to accept the terms of the license agreement; the **Choose Destination Location** screen displays.
4. Specify your own directory, or accept the default destination location and click "Next" to continue; the **Select Components** screen displays.



5. Select the components that you want to install and press "Next" to continue. The **Select Program Folder** screen displays.
6. Accept the default, or specify another location and click "Next" to continue; the **Check Setup Information** screen displays.
7. Click "Next" to perform the installation. When finished, the **Setup Complete** screen displays. If you want to install the ASG Soft Key on a supported handheld, select "Launch Palm/BlackBerry install programs" and proceed to Section 2.3. Select "Launch ASG Soft Key for Windows" to begin using the Windows token. Click "Finish" to exit the installation software.

2.2 Installing the ASG Soft Key on a Handheld Device

This section provides instructions for installing the ASG Soft Key on either a Palm™ or RIM BlackBerry using the installation software that accompanies each device. The ASG Soft Key currently supports the following versions of these mobile operating platforms:

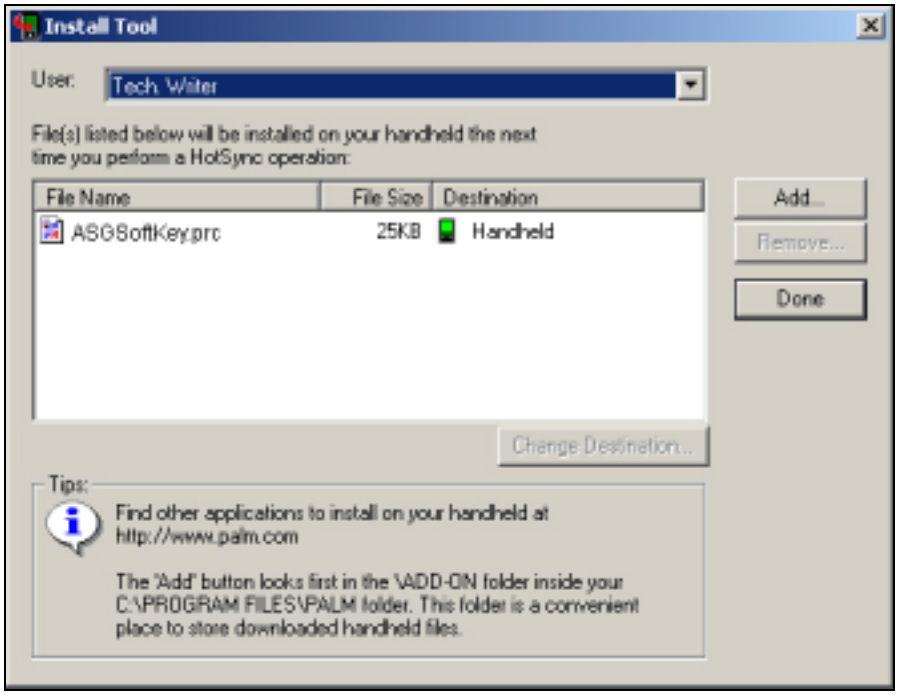
- Palm OS® for Palm™ handhelds: versions 3.5 and 4.0
- RIM BlackBerry™ wireless handhelds: versions 2.0 and 2.1

You will need the desktop installation software that accompanied your handheld to install the ASG Soft Key.

➔	These instructions pertain to the installation of the ASG Soft Key on a handheld. For detailed software installation instructions, refer to the user documentation that accompanied your device.

2.2.1 Palm™ Handheld Installation

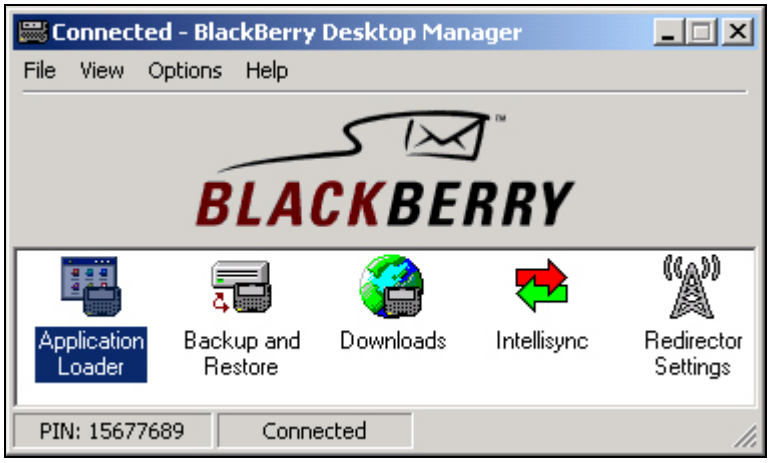
1. When the Palm Desktop software is launched, the **Install Tool** screen displays the "ASGSoftKey.prc" file that you will download to your Palm™ handheld.



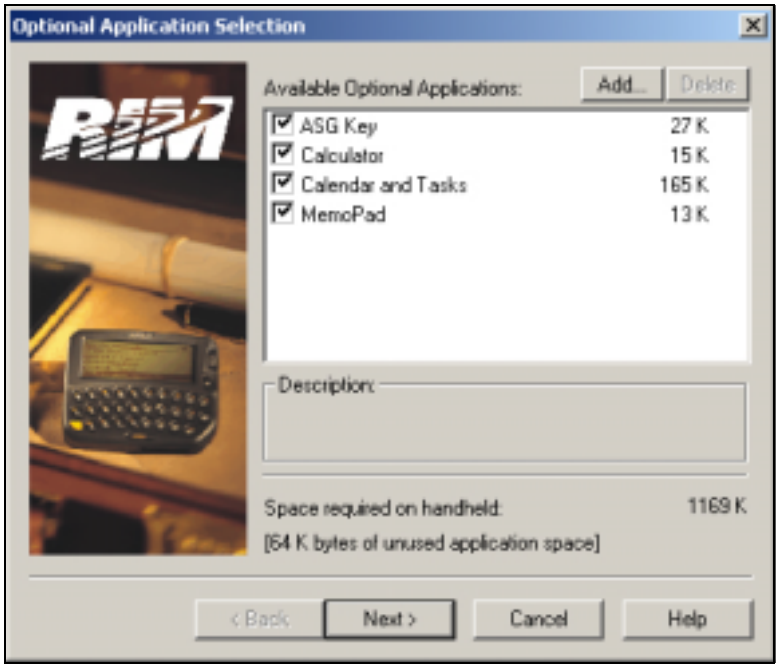
2. Press "Done" to close the **Install Tool**; the ASG Soft Key software is stored in the default Add-On Folder located in the Palm Desktop directory. The next time you perform a HotSync operation, the program will be automatically installed on your handheld. Press "OK".
3. Cradle your handheld and press the HotSync® button. The handheld's screen displays progress indicators as the application is being added to the device.

2.2.2 BlackBerry™ Wireless Handheld Installation

1. Whether you launched the BlackBerry™ Desktop Manager software at the end of the ASG Soft Key Windows installation, or you opened the program from your computer's desktop, the **BlackBerry Desktop Manager** screen displays.



2. Make sure that your BlackBerry™ wireless handheld is seated in its cradle and double-click the "Application Loader" icon; the **Welcome to Application Loader** screen displays.
3. Press "Next" to proceed with the installation. Once the Desktop Manager reads the configuration of your handheld, the **Optional Application Selection** screen displays.



4. Check the ASG Soft Key box and press "Next" to continue; the **Unused Application Space** screen displays. Select an option and press "Next;" the **Existing Data Preservation** screen displays. Select an option and press "Next;" the **Summary** screen displays.
5. Press "Finish" to start the loading process. A progress bar indicates the status of the download, and a prompt displays when the installation is complete.

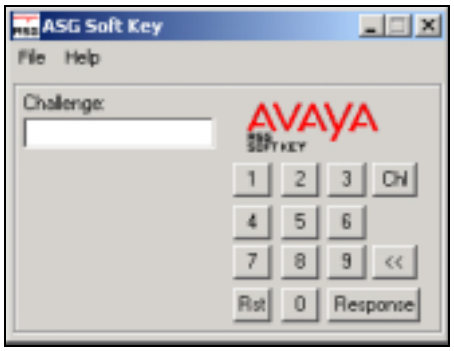
2.3 ASG Soft Key Feature Overview

Now that you have installed the ASG Soft Key, you can familiarize yourself with its interface and features. This section provides an overview of the ASG Soft Key's features, as well as illustrates the difference between the supported operating platforms.

2.3.1 The ASG Soft Key Interface

The following graphics illustrate the ASG Soft Key interface for all available platforms.

ASG Soft Key for Microsoft Windows

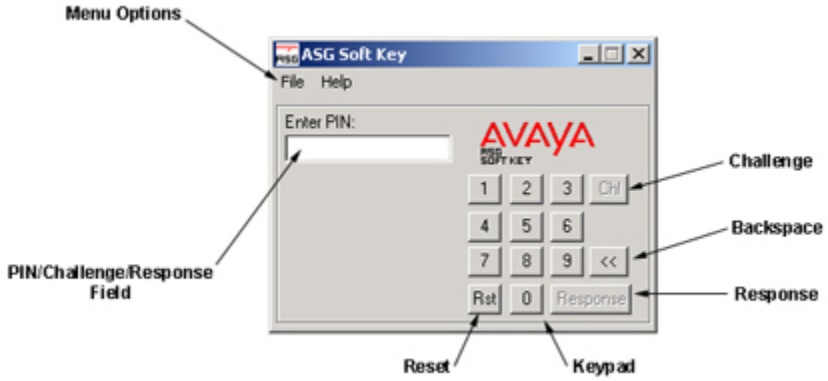


ASG Soft Key for Palm™ Handhelds

ASG Soft Key for BlackBerry™ Wireless Handhelds

2.3.2 ASG Soft Key Features

This section describes the physical features of the ASG Soft Key.



PIN/Challenge/Response Field – In PIN mode, enter your PIN to log into the token. In authentication mode, you can enter challenges and receive responses.

➔	For all operating platforms, the session expires and returns to the PIN prompt after 60 seconds of inactivity.

Rst (Reset) – Press this button to force your current session to close and return to the PIN prompt.

Continued on next page

ASG Soft Key Features, continued

Keypad – Use the mouse, or press the corresponding keys on your computer's keyboard, to enter your PIN and challenges, as well as request responses.

Response – Press this button to generate a response.

<< (Backspace) – Press this button to erase your PIN, or challenge entries one character at a time.

Chl (Challenge) – Press this button to display the Challenge prompt. This field automatically displays after you enter your PIN.

Menu Options – Choose from "Configure" and "Exit"

- *Configure* –Specify your PIN, and Key.
- *Exit* – Closes the application.

3. Configuring Your ASG Soft Key

Now that you have installed the software, and familiarized yourself with its interface and features, you can configure your token with your PIN and Key.

About Your "PIN" Your *PIN* can contain 4 to 8 numeric characters, and is a value that you can change at any time. You must remember this number so that you can access your software token.

About Your "Key" Your *Key* is a unique (secret) value that is associated with the login profile in the destination appliance. Either you, or the administrator of the destination appliance creates a user profile that identifies the ASG Key authentication mode. At that time, a key is either randomly generated by the appliance, or a user-defined key is entered into the appliance.

This section provides brief instructions for adding a user profile to a destination appliance, and configuring the ASG Soft Key for first time use. For detailed information on adding users to ASG Guards, refer to the documentation that accompanied the appliance.

3.1 Creating a User Profile on a Destination Appliance

These instructions assume that you can access the appliance either through a preset login using one of the supported authentication methods, or can physically connect to the device through the AUX port using the default login that does not require authentication.

If you are not responsible for adding users, or do not have access rights to add user profiles for yourself or others to the device, you should obtain your key from the administrator of the device, and can skip ahead to **Section 3.2: Configuring Your ASG Soft Key**.

To create a user profile:

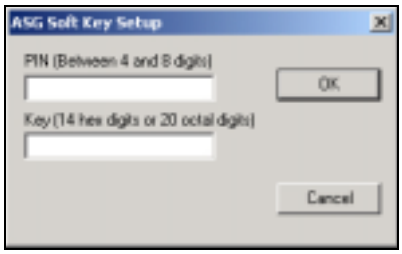
1. Log into the destination appliance.
2. Depending on the type of user you are defining, enter the command AU or AAU. The **--- Add User ---** dialog displays.
3. Specify your choices for the following parameters: *access class*, *concurrent logins*, *logging session activity*, *block access*, *sessions allowed*, and *user expiration date*.
4. For the *Primary Authentication Method* parameter, use the SPACE key to select **ASG Key**. Repeat this step to select a *Secondary Authentication Method*, if appropriate.
5. If desired, enter any auto execute commands or options. The --- ASG Key Details --- dialog displays.
6. Define the key with which you will seed the ASG Soft Key by selecting one of the following *Encryption Key Sources*:
   - Randomly Generated: appliance-defined unique key
   - Fixed: user-defined unique key

   Press ENTER after you have made your selection. You will be prompted with a test challenge that you will use when seeding the ASG Soft Key. Do not clear this screen until you have configured your token. Proceed to **Section 3.2: Configuring Your ASG Soft Key**.

3.2 Configuring Your ASG Soft Key

For all platforms, when the ASG Soft Key is launched for the first time, the **ASG Setup** screen displays.

Windows



Palm™

BlackBerry™

To configure your settings:

1. Specify a 4 to 8 digit numeric PIN.
2. Enter the 20-digit octal Key This value should match the value entered in (Fixed) or display within (Randomly Generated) your user profile of the destination equipment.
3. To save your settings do one of the following:
   - Windows: press “OK”
   - Palm™ handhelds: press “Save”
   - BlackBerry™ wireless handhelds: press the roller wheel and select “Save” from the menu list

Once you have configured your software token, you can access the **ASG Setup** screen at any time to change your settings by doing one of the following:

- Windows: Select File > Configure.
- Palm™ handhelds: Tap ASG > File > Configure.
- BlackBerry™ wireless handhelds: Press the roller wheel and select “Configure.”

➔	You can change your PIN at your discretion. **DO NOT** change your KEY unless you or your System Administrator makes the same change to your user profile on the destination appliance, or you will not be able to log in.

3.3 Testing Your Configuration

Whenever you add a user profile for an ASG Soft Key, you will be presented with a test challenge to confirm that you have configured your token correctly (see step #6 of section 3.1).

To test your configuration:

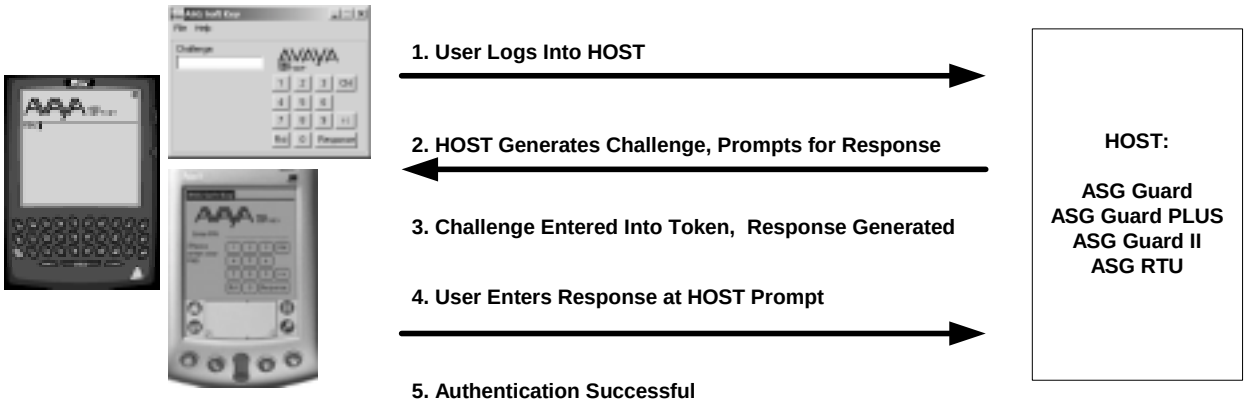
1. Enter your PIN into the ASG Soft Key – the **Challenge** prompt displays.
2. Enter the test challenge in the Challenge field and press the Response button. The token generates a Response. The number that displays in the Response field should match the response displayed on the destination equipment.

➔	If the response on your token does not match the test response, either the user profile on the Guard or the token itself is programmed with incorrect an user key. Confirm the keys match on the destination and token. Contact the administrator of the device for assistance if necessary.

4. Using the ASG Soft Key

4.1 Authentication Overview

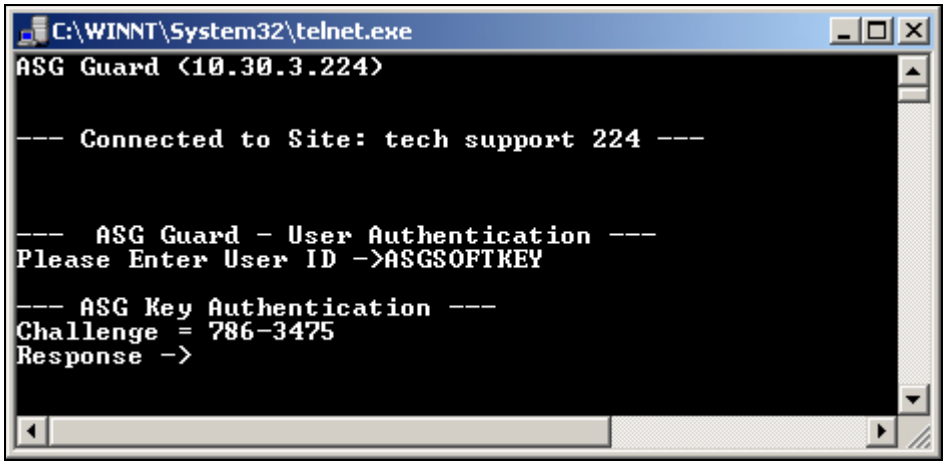
The diagram below illustrates the authentication process between the ASG Soft Key and destination appliances.



4.2 Authenticating to ASG Series Appliances

This section provides instructions for authenticating to an ASG Series appliance.

1. At the command prompt of any telnet, serial, or modem connection, type your User ID and press ENTER; the **ASG Key Authentication** dialog displays a challenge.



2. Enter your PIN into the ASG Soft Key; the “Challenge” field automatically displays.

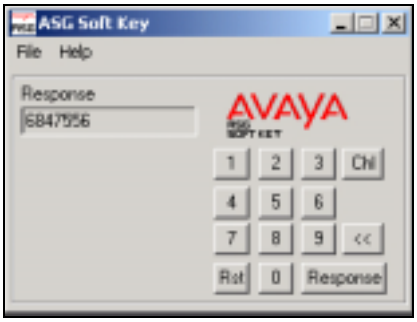
Continued on next page

Authenticating to ASG Series Appliances, continued

3. Enter the challenge from the appliance into the software token and retrieve your response by either pressing the “Response” button or selecting “Response” from the menu.

➔	If you are using ASG Soft Key for Windows, you may cut-and-paste the response code into your terminal window, instead of typing it manually.

Windows



Palm™

BlackBerry™

4. Use the response to log in to the appliance.

➔	After three consecutive failed attempts the session is terminated. Contact the System Administrator for assistance with determining that the user key on your software token matches your user profile.